



CENTER FOR TRUSTWORTHY  
SCIENTIFIC CYBERINFRASTRUCTURE  
The NSF Cybersecurity Center of Excellence

# Today and Tomorrow: CTSC's Services and Vision

---

Von Welch, CTSC PI and Director  
Jim Basney, Craig Jackson, Barton Miller, Jim Marsteller,  
Co-PIs

NSF Cybersecurity Summit  
August 16th 2017

---

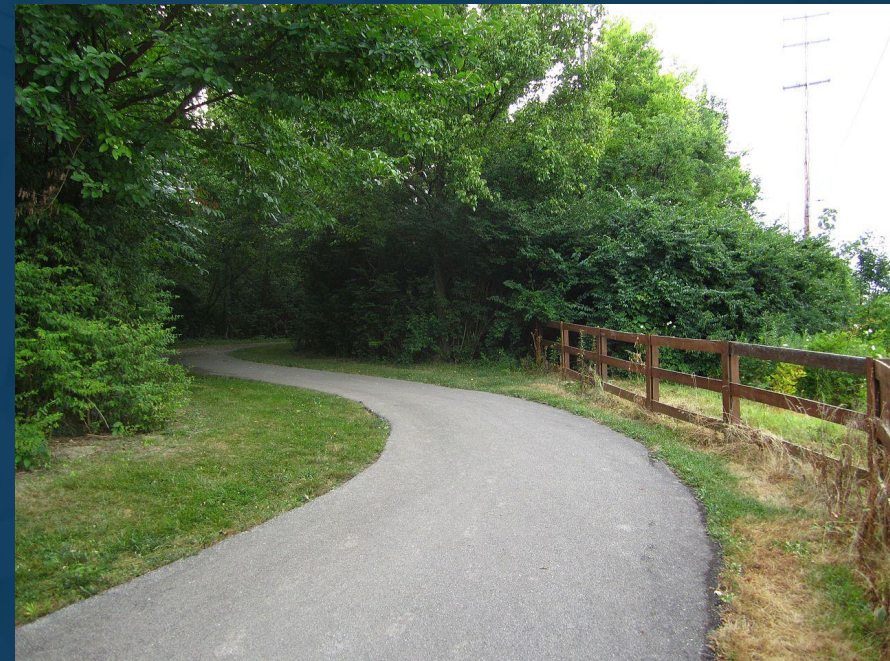
<http://hdl.handle.net/2022/21720>

[trustedci.org](http://trustedci.org)

# Talk Outline

---

- The Value of Cybersecurity to Science
- Today: CCoE services to the NSF Community
- Progress and Looking Ahead



# The Value of Cybersecurity to Science

---



# Trusted and Reproducible Science

News Magazine Advanced LIGO LIGO science Educational resources

latest news news archive upcoming events press releases press information

## "BLIND INJECTION" STRESS-TESTS LIGO AND VIRGO'S SEARCH FOR GRAVITATIONAL WAVES

The LIGO Scientific Collaboration and the Virgo Collaboration completed an end-to-end system test of detection capabilities at their recent joint collaboration meeting in Arcadia, CA. Analysis of data from LIGO's most recent observation run revealed evidence of the elusive signal from a neutron star spiral black hole. The collaboration knew that the "detection" could be a "blind injection" — a fake signal added to data without telling the analysts, to test the detector and analysis. Nonetheless, the collaboration proceeded under the assumption that the signal was real, and wrote and approved a scientific paper reporting the breaking discovery. A few moments later, according to plan, it was revealed that the signal was indeed an injection.

While the scientists were disappointed that the discovery was not real, the success of the analysis was a compelling demonstration of the collaboration's readiness to detect gravitational waves. LIGO and Virgo scientists are looking forward to observations with the advanced detectors which are expected to continue in 2015.

CMS People Detector Physics Education and Outreach Jobs Contact

### About CMS

- What is CMS?
- CMS Physics
- Recipe for a Universe
- Story of the Universe
- The size of things
- The Big Questions

## Blinding and unblinding analyses

CMS performs searches for new particles by looking for signals amidst a background of known physics. If the data are something more interesting than expected in a certain region, CMS is to make sure that the results are not significantly affected by the background.

Understanding Science how science really works

Support this project

search | glossary | home

## The science checklist applied: Cold fusion

Fusion occurs when two light atoms, like hydrogen, join together, or fuse, into a single heavier atom, releasing a lot of energy in the process. In 1989, chemists Stanley Pons and Martin Fleischmann excited the world with claims that they had produced fusion at room temperature — "cold" fusion compared to the high temperatures the process was thought to require. Their discovery seemed to offer a potential solution to the energy crisis: cheap energy, without pollutants or radioactive waste.

Science cannot be absolutely defined; however, scientific endeavors have a set of key characteristics, summarized in the Science Checklist.

Home | News & Comment | Research | Careers & Jobs | Current Issue | Archive | Audio & Video | For Authors

News & Comment | News | 2016 | February | Article

NATURE | NEWS

## Biotech giant publishes failures to confirm high-profile science

Amgen posts three studies at new online channel for discussing reproducibility.

Monya Baker

04 February 2016

Rights & Permissions

A biotechnology firm is releasing data on three failed efforts to confirm findings in high-profile scientific journals — details that the industry usually keeps secret.

Amgen, headquartered in Thousand Oaks, California, says that it hopes the move will encourage others in industry and academia to describe their own replication attempts, and thus help the scientific community to get to the bottom of work that other labs are having trouble verifying.

The data are posted online at a newly launched channel dedicated to quickly publishing efforts to confirm scientific findings. The 'Preclinical Reproducibility and Robustness' channel is hosted by F1000Research, the publishing platform of London-based publishers Faculty of 1000 (F1000).

Scientists who are concerned about the irreproducibility of preclinical research say that they welcome the initiative — but are not sure whether it will gain traction.

### Smooth moves

Meet the soft, cuddly robots of the future

Rigid robots step aside — a new generation of squishy, stretchy machines is wiggling our way.

Like Share 231,004 people like this. Sign Up to see what your friends like.

Recent Read Commented

- Tasmanian bushfires threaten iconic ancient forests Nature | 04 February 2016
- Forests not equal when it comes to climate Nature | 04 February 2016
- Humour on the brain: Robert Newman reviewed Nature | 04 February 2016

## theoretical ecology

Notes from ecology, biogeography and evolution by Peter Hargis

About me RSS feed Twitter @TheorEcology Ecology Jobs

## Statistical analysis with blinded data — a way to go for ecology?

Peter Hargis | June 22, 2014

In my [last post](#) about the Higgs rumors, I referred to an [exchange](#) between Ben and Peter Woit about the significance of seeing information about the experimental results before the data analysis has been completed. One thing that made me thinking was Woit's point about "blinding the data". From the context, I could understand what they referred to, but confirming my hunch on Woit's point made me aware how common such a blinding analysis seems to be in particle physics. From the article about [blind analysis](#).

Justitia, 1556, by Maarten van Heemskerck

Most accessed

- 04 2012 proposed factors for the loss of biodiversity
- A simple Metabolic Network, MCMC, and
- MCMC, chain analysis, and
- 04 2012 proposed factors for the loss of biodiversity
- 04 2012 proposed factors for the loss of biodiversity
- 04 2012 proposed factors for the loss of biodiversity
- 04 2012 proposed factors for the loss of biodiversity
- 04 2012 proposed factors for the loss of biodiversity

Recent Comments



# Do No Harm

NSF CI represents some impressive computing, networking, and data.

Keeping it available and preventing its use to harm others are **key to our productivity and reputation.**



# Enabling Collaboration

---

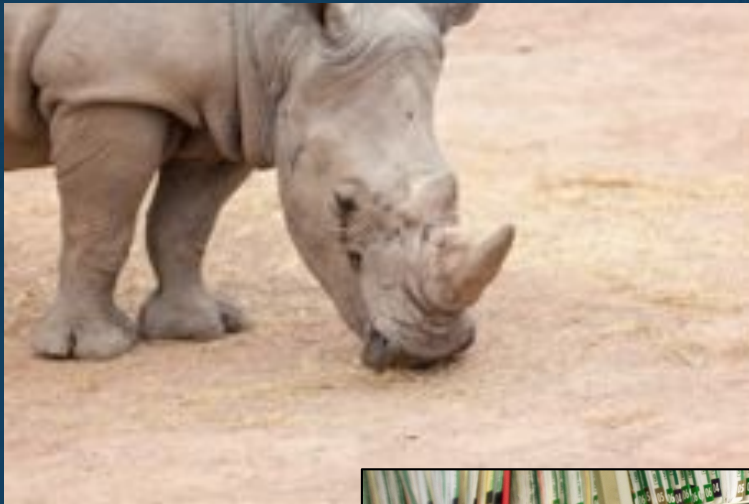
NSF science is increasingly collaborative - both inter-organizational and inter-disciplinary.

Security plays a role, sometimes subtle, in **enabling collaboration** between projects and organizations.



# Science Domain and Project Concerns

## (Yes, even for open science projects)



### About The LIGO Gravitational-Wave Rumor. . .

By: Shannon Hall | January 13, 2016



*The physics and astronomy world is all agossip: has LIGO heard its first black-hole merger? Well, not so fast.*

Rumors are swarming on social media that the newly upgraded LIGO, the Advanced Laser Interferometer Gravitational-Wave Observatory or aLIGO, has finally seen the gravitational-wave signature

stellar-mass black holes colliding together and merging. Maybe even two black holes since the first observation. Or not.

Observation would be one of the most important predictions of Einstein's general theory of relativity, and it would also open a new field of cosmic observation: gravitational-wave astronomy.



LIGO consists of two L-shaped interferometers, one in Hanford, Washington (shown here), and one in Livingston, Louisiana. Each arm of each L is 2½ miles (4 km) long. Lasers look for changes in each arm's length as small as a thousandth the diameter of a proton. Passing gravitational waves might distort space-time by that much. *LIGO Laboratory*

<http://www.skyandtelescope.com/astronomy-news/about-this-weeks-gravitational-wave-rumor/>



# CCoE services to the NSF Community

---

# Center for Trustworthy Cyberinfrastructure

## The NSF Cybersecurity Center of Excellence

---

### Mission

Provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.



Andrew Adams, Kay Avila, Jim Basney, Robert Cowles, Jeannette Dopheide, Terry Fleury, Grayson Harbour, Randy Heiland, Elisa Heymann, Craig Jackson, Scott Koranda, Mark Krenz, Jim Marsteller, Prof. Barton Miller, Warren Raquel, Susan Sons, Amy Starzynski Coddens, Von Welch, John Zage

<http://trustedci.org/who-we-are/>





# CCoE Thrusts

---

## **Building Community**

NSF Cybersecurity Summit, Monthly Webinars, Blog, Email Lists, Partnerships, Benchmarking Survey

## **Sharing Knowledge**

Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects, Identity Management Best Practices, Cyberinfrastructure Vulnerabilities, Training, OSCRP

## **Collaboration to Tackle Challenges: Engagements**

LIGO, SciGaP, IceCube, Pegasus, CC-NIE peer review, DKIST, LTERNO, DataONE, SEAD, CyberGIS, HUBzero, Globus, LSST, NEON, U. Utah, PSU, OOI, Gemini, Array of Things, IBEIS, SciGaP, US Antarctic Program...

# Collaboration to Tackle Challenges: Engagements

---

# Engagements

Focused collaborations with one (or small group) of NSF projects to tackle a project's cybersecurity or identity and access management challenge.

## Two important challenges (among many)

### Cybersecurity and policy

- On premise services, potentially managed by third parties, present additional risks that need to be understood
  - Engagements with CISO from our campuses
  - Engagement with Center for Trustworthy Scientific Cyberinfrastructure

### Scientific outreach

- Underlayment to Science
  - Embedded with science collaborations with multi-institution cyberinfrastructure - distributed data services, software, job routing
  - Developers associated with the Science Gateways Community Institute



## TrustedCI.org Peer Review with Utah



- <http://trustedci.org/cc-nie/>
- We Discussed:
  - Problems or Research bottlenecks
  - Design
  - Architecture
  - Host, Data, Network Security
- I HIGHLY recommend this.
- Contact CTSC Director Von Welch(vwelch@iu.edu) at the Center for Trustworthy Scientific Cyberinfrastructure



globus.org

Secure means all resources are protected

Globus service is itself highly secure

✓ Best-practice cloud security

✓ Third-party security reviews



Globus platform ensures your services are secure

✓ Accept credentials from 300+ identity providers

✓ Control proxy credential lifetimes

✓ Industry-standard OAuth-2 and OIDC protocols

✓ Data encryption

✓ Build secure services with controlled delegation

Accessible

Ubiquitous

Performant

Secure

Reliable

Programmable

Manageable

Sustainable



# Any challenge is in scope!

Any Cybersecurity-related  
challenge in scope:

Drafting a Privacy Policy (AoT)

Security Officer search (LIGO)

Identity and Access

Management:

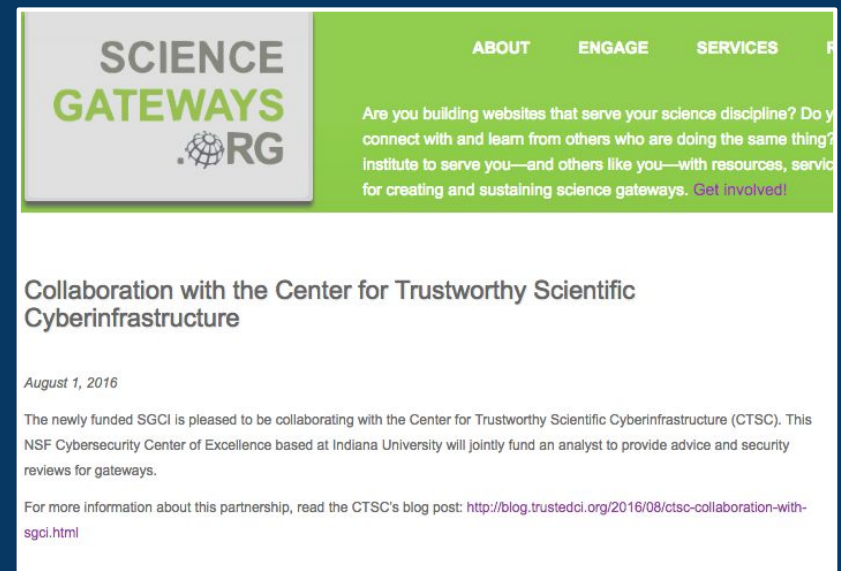
<http://trustedci.org/iam/>

Software Assurance:

<http://trustedci.org/software-assurance/>

Science Gateways  
w/SGCI SI2 Institute:

<http://sciencegateways.org/news/collaboration-ctsc/>



# Apply now!

Current deadline for  
first half of 2018 is  
**October 2nd.**

Demand was 2x  
supply in last  
application window.

QUESTIONS

RESPONSES 3

## CTSC Engagement Application

Please complete all items and submit your application. If you have questions about this form or CTSC engagement processes, please see <http://trustedci.org/application>.

Do NOT put sensitive information of any kind into this form. If you have any questions about this form, contact [info@trustedci.org](mailto:info@trustedci.org).

---

### Project or Facility Information

Description (optional)

1. Project or facility name \*

Short answer text

2. Provide the source of funding (NSF directorate(s) or other) with award numbers. \*

<http://trustedci.org/application>

# Sharing Knowledge

## Guides, Best Practices, Situational Awareness, Training

---



# CI Vulnerability Alerts - Situational Awareness

---

Advise NSF CI community about **relevant software vulnerabilities** and provide guidance on mitigation.

Leverage NIST, US-CERT, EGI, OSG, XSEDE, REN-ISAC, and other sources of vulnerability information.

**Subscribe** to [cv-announce@trustedci.org](mailto:cv-announce@trustedci.org) for alerts.

**Contact** [alerts@trustedci.org](mailto:alerts@trustedci.org) to report vulnerabilities.

[trustedci.org/vulnerabilities](https://trustedci.org/vulnerabilities)

# Cybersecurity Guides and Tools

Addressing concerns **unique to science**  
Operational Security (policy templates,  
guidance, etc.)

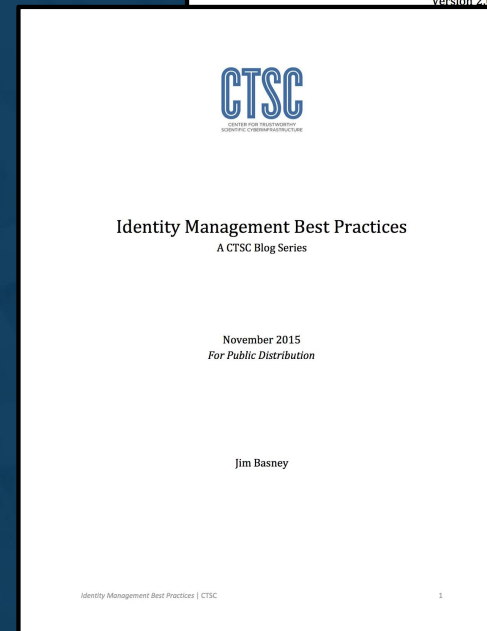
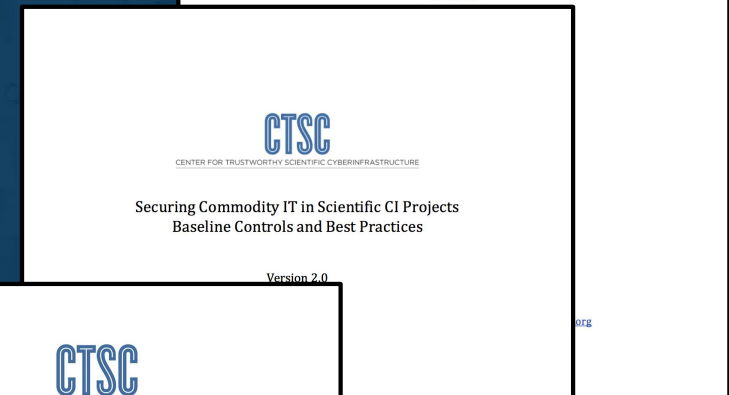
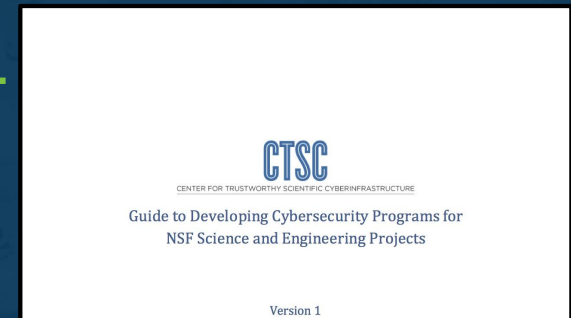
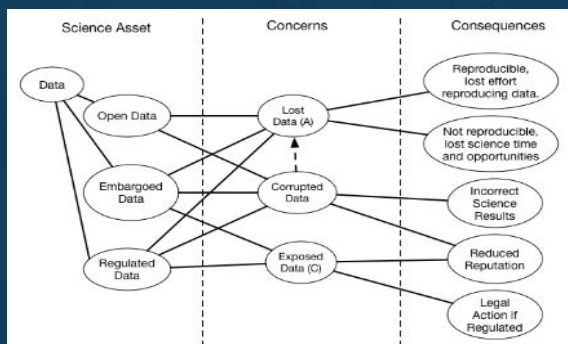
<http://trustedci.org/guide>

Identity Management Best Practices

<http://trustedci.org/iam>

Open Science Cyber Risk Profile

<https://trustedci.org/oscrp/>





CENTER FOR TRUSTWORTHY  
SCIENTIFIC CYBERINFRASTRUCTURE  
The NSF Cybersecurity Center of Excellence

Home

About CTSC

+

Getting Help From CTSC

Engaged Communities

+

Community Resources

+

Training

-

Online Training

Training Materials

## Training materials

2016 Spring Practical Cybersecurity for Open Science Projects

2015 NSF Cybersecurity Summit Training Materials (August 17, 2015)

- Bro Platform Training Workshop - Johanna Amann (ICSI), Justin Azoff (NCSA) & Adam Slagell (NCSA)
- Developing Cybersecurity Programs for NSF Projects - Bob Cowles, Craig Jackson, Jim Marsteller & Susan Sons (CTSC)
- Vulnerabilities, Threats, and Secure Coding Practices - Barton P. Miller & Elisa Heymann
- Industrial Control Systems, Networking, and Cybersecurity - Phil Salkie (Jenariah Industrial Automation)
- Aligning your Research Cyberinfrastructure with HIPAA and FISMA - Anurag Shankar (Indiana University)
- Incident Response Training - Randy Butler (NCSA)

2014 NSF Cybersecurity Summit Training Materials (August 26, 2014)

- Developing Cybersecurity Programs for NSF Projects (PDF) - Jim Marsteller, Susan Sons, Craig Jackson, Jared Allar (CTSC)
  - Also available as a series of online videos
- Vulnerabilities, Threats, and Secure Coding Practices (PDF) - Barton P. Miller, James A. Kupsch, Elisa Heymann (University of Wisconsin)
- HPC, HIPAA, and FISMA: Meeting the Regulatory Challenge through Effective Risk Management (PowerPoint) - Bill Barnett & Anurag Shankar (Indiana University)
- Incident Response Training (Powerpoint part 1, Powerpoint part 2) - Randy Butler, Warren Raquel, Patrick Duda (NCSA)

NSF Cybersecurity Summit, XSEDE, SuperComputing, **other locations by request.**

Topics: Cybersecurity Program Development, Incident Response, Secure Coding, Software Engineering...

<http://trustedci.org/trainingmaterials/>

# Building Community

## NSF Cybersecurity Summit, Webinars, Blog, Email Lists, Partnerships

---



# Large Facility Security Team

---

- Monthly virtual meetings facilitated by CTSC
- Topical discussions and opportunities to bring questions and issues to the table
- Current participation: 15 of 25 LFs
- Provide feedback and input on the Cybersecurity subsection of the Large Facilities manual
- Provide critical input on LF software requirements for software producers

# CTSC Webinar Series

[\*trustedci.org/webinars\*](https://trustedci.org/webinars)

---

## *Upcoming:*

- *Aug 28: Two-Factor Authentication for CI*
- *Aug 30: CTSC Engagement Application Process*
- *Sep 25: Threat Intelligence Sharing*

*Average # of Viewers: 35 live, 65 later on YouTube*

*Call for presentations: [\*trustedci.org/webinars-cfp\*](https://trustedci.org/webinars-cfp)*

# Partnerships

---

**Interoperability with** and **best practices** from our global collaborators.

**ESnet**: Open Science Cyber Risk Profile

**AARC**: Identity Management with the EU

**SGCI SI2 Institute**: Science Gateway cybersecurity

**Bro CoE**: Training, network security

**REN-ISAC**: Situational Awareness

<http://trustedci.org/partners/>

# Your Input Requested!

## 2017 NSF Community Cybersecurity Benchmarking Survey

---

Goals: Give the community a richer understanding of the environment and norms; additionally, provide a long-term measurement of our community's cybersecurity stance.

Annual community survey open to all NSF projects.

Reports capture each year's results.

Only contain information to maintain anonymity to respondents.

2016 survey report: <http://hdl.handle.net/2022/21355>

Note: ALL respondents said that they developed software.

2017 survey now open: [trustedci.org/survey](https://trustedci.org/survey)



## Staying in contact with the CCoE

---

Got a quick question?  
[ask@trustedci.org](mailto:ask@trustedci.org)

Join our email lists for discussions and updates:  
<http://trustedci.org/ctsc-email-lists/>

Blog: <http://blog.trustedci.org/>

 Twitter: [@TrustedCI](https://twitter.com/TrustedCI)

# Progress and Looking Ahead

---

# Vision for the NSF Science Community

---

1. For the NSF science community to **understand fully the role of cybersecurity in producing trustworthy science.**
2. For all NSF projects and facilities to **have the information and resources they need to build and maintain effective cybersecurity programs** appropriate for their science missions, and responsive to evolving risks and requirements.
3. For **all NSF Large Facilities to have highly effective cybersecurity programs.**

# Progress and Looking Ahead

---

**Progress:** A baseline cybersecurity program for a mature, operational CI project has clear components.

**Progress/Looking Ahead:** Expectations for secure software development / engineering are emerging.

**Looking Ahead:** Enable campus infosec to help research with the same strength they help enterprise.



## Progress:

A baseline cybersecurity program for a mature, operational CI project has clear components.

---

# PILLARS OF A CYBERSECURITY PROGRAM

## BASE EXPECTATIONS OF A MATURE CI

---

### 1. GOVERNANCE

*Roles, Processes, Policies, Requirements*

### 2. RESOURCES

*People, Infrastructure, and Security Tools...  
Money*

### 3. CONTROLS

*Procedural, technical, administrative  
safeguards and countermeasures*

# PILLARS OF A CYBERSECURITY PROGRAM

## BASE EXPECTATIONS OF A MATURE CI

---

### 1. GOVERNANCE

*Roles, Processes, Policies, Requirements*

#### Base Expectations:

- Leadership Engagement: clear responsibility for cybersecurity - PI or delegate.
- Master Information Security Policy and Procedures (MISPP)
- Acceptable Use Policy (AUP)
- Incident Response Policies & Procedures
- Access Control Policy

# PILLARS OF A CYBERSECURITY PROGRAM

## BASE EXPECTATIONS OF A MATURE CI

---

1. Invest in people
2. Give them a budget

## 2. RESOURCES

*People, Infrastructure, and Security Tools...  
Money*

Cybersecurity budgets: 3% to 12% of IT budgets.  
(Higher for smaller projects.)

See 2016 NSF Cybersecurity Summit Report for details:

<http://hdl.handle.net/2022/21161>



# PILLARS OF A CYBERSECURITY PROGRAM

## BASE EXPECTATIONS OF A MATURE CI

1. Select a reasonably scoped, prioritized, and evidence-based baseline control set.  
E.g. CIS Critical Security Controls (aka the Top 20).
2. Determine the relevance, feasibility, and current implementation state of these controls.
3. Fill gaps (unique/unusual science CI) with analysis-based controls.  
E.g. <https://trustedci.org/oscrp/>

### 3. CONTROLS

*Procedural, technical, administrative safeguards and countermeasures*

# PILLARS OF A CYBERSECURITY PROGRAM

## BASE EXPECTATIONS OF A MATURE CI

---

### 1. GOVERNANCE

For more information see:

<http://trustedci.org/guide>

"Beyond the Beltway" talk this afternoon.

safeguards and countermeasures

## Progress/Looking Ahead:

Expectations for secure software development / engineering are emerging.

---

# Emerging Expectations for Secure Software Development: **Basic Expectations**

---

Basic secure software development expectations have emerged.

E.g. basic engineering practices:

- Versioning
- Design for security
- Vulnerability management
- Patch release
- Developer awareness of security.

For more  
information see:

[https://trustedci.org/  
software-assurance/](https://trustedci.org/software-assurance/)

Todd Tannenbaum's  
talk



# Emerging Expectations for Secure Software Development: **See Also**



SOFTWARE EVALUATION: CRITERIA-BASED  
NOVEMBER 2011

## **Software Evaluation: Criteria-based Assessment**

Mike Jackson, Steve Crouch and Rob Baxter

*Criteria-based assessment is a quantitative assessment of the software in terms of sustainability, maintainability, and usability. This can inform high-level decisions on specific areas for software improvement.*

A criteria-based assessment gives a measurement of quality in a number of areas. These areas are derived from *ISO/IEC 9126-1 Software engineering — Product quality*<sup>1</sup> and include usability, sustainability and maintainability.

The assessment involves checking whether the software, and the project that develops it, conforms to various characteristics or exhibits various qualities that are expected of sustainable software. The more characteristics that are satisfied, the more sustainable the software. Please note that not all qualities have equal weight e.g. having an OSI-approved open source licence is of more importance than avoiding TAB characters in text files.

<https://www.software.ac.uk/resources/guides-everything/software-evaluation-guide>

# Emerging Expectations for Secure Software Development: **Challenges**

---

- What's the right budget for software security?
- Which assurance tools to use (SAST, DAST, code review, etc.) and when?
- How to assess risk on large code bases?
- How do you verify what a software developer is doing or did with regards to security?
- How to deal with third party software of unknown risk?

**Very large challenge.** Need help from private sector, cybersecurity research, ... everyone to address.

# Emerging Expectations for Secure Software Development: Example Work in this Area

<https://www.bsimm.com/>

TWELVE CORE ACTIVITIES “EVERYBODY” DOES	
ACTIVITY	DESCRIPTION
[SM1.4]	Identify gate locations and gather necessary artifacts
[CP1.2]	Identify PII obligations
[T1.1]	Provide awareness training
[AM1.2]	Create a data classification scheme and inventory
[SFD1.1]	Build and publish security features
[SR1.2]	Create a security portal
[AA1.1]	Perform security feature review
[CR1.4]	Use automated tools along with manual review
[ST1.1]	Ensure QA supports edge/boundary value condition testing
[PT1.1]	Use external penetration testers to find problems
[SE1.2]	Ensure host and network security basics are in place
[CMVM1.2]	Identify software bugs found in operations monitoring and feed them back to development

<https://continuousassurance.org/>



## Looking Ahead:

Enable campus infosec to help research with the same strength they help enterprise.

---

# NSF's CI Community Scale

---

In 2016, NSF made over >300k awards

Over 500 awards were to \$1m+ projects

<https://www.nsf.gov/awardsearch/advancedSearch.jsp>

Assuming 3-5 year awards and some CI in \$1m+ projects, estimate **2000 CI projects currently funded.**

To impact security across this many projects, CTSC needs a force multiplier.



# Can Campus Infosec be that **Force Multiplier**?

---

Information Security (infosec) officers on campus are primarily focused on enterprise computing (cloud or on-prem), followed by regulated data (HIPAA, 800-171, FISMA, FERPA, etc.)

Open Science is heterogeneous, relatively fast moving, and has varying risks and rewards.

These factors makes it **hard for campus infosec and CI to engage.**

# The Path Forward

---

Despite challenges, campus infosec seems the best available force to help meet scale of NSF science.

Need to educate and train them in cybersecurity for NSF science, both the **How** and the **Why**.

## **Strategy:**

Start with “early adopters” - campuses embracing research computing strongly - and let them spread the word to their peers.

# In Conclusion

---

Cybersecurity for science is critical: trustworthiness, preventing harm, collaboration, etc.

We're here to help: <https://trustedci.org/help/>

Cybersecurity programs have base expectations

Software security expectations are emerging.

Scaling to size of NSF science is a challenge, look to engage with campus infosec.



CENTER FOR TRUSTWORTHY  
SCIENTIFIC CYBERINFRASTRUCTURE  
The NSF Cybersecurity Center of Excellence

Thank You

[trustedci.org](https://trustedci.org)

---

We thank the National Science Foundation (grant 1547272) for supporting our work.

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.